DOI: 10.52694/ThPSR.124.3

Elżbieta Posłuszna
Anna Turner

System penitencjarny w świecie zdepersonalizowanych inicjatyw haktywistycznych

The penitentiary system in the world of depersonalized hacktivist initiatives

Sieciowy charakter zglobalizowanego społeczeństwa oraz rozwój nowych technologii utorował drogę cyberkonfliktom. Kiedy po jednej stronie zaangażowane w walkę są siły niehierarchiczne, sieciowe, często zorganizowane na wzór oporu bez przywództwa i zespolone za sprawą walczących idei w sieć internetową, trudno sobie z nimi poradzić, zwłaszcza za pomocą klasycznych, hierarchicznych struktur organizacyjnych. W artykule realizujemy dwa cele. Pierwszym jest analiza taktyki głównych aktorów cyberkonfliktów – grup i jednostek parających się atakami na system penitencjarny i działających w dwóch wymiarach: defensywnym (wykorzystującym przecieki informacji) oraz ofensywnym (wykorzystującym sabotaż). Taktykę pierwszego rodzaju omawiamy na przykładzie WikiLeaks oraz grupy Edaalate Ali, taktykę drugiego rodzaju na przykładzie grupy antykremlowskich haktywistów. Cel drugi sprowadza się do przedstawienia owych działań w szerszej perspektywie walki sieciowej oraz zaproponowania zarysu strategii zawiadywania aktywnościami tego rodzaju aktorów, co miałoby się dokonać w oparciu o sieciowe „sterowanie motywacjami", czyli propagandowe pobudzanie do określonych postaw i sieciowych działań oddolnych.

Słowa kluczowe: walka sieciowa, opór bez przywództwa, system penitencjarny, haktywizm, WikiLeaks, Edaalate Ali

The networked nature of globalized society and the development of new technologies has paved the way for cyberconflicts. When

non-hierarchical, networked forces are involved on one side, often organised along the lines of leaderless resistance and fused through warring ideas into an online network, they are difficult to deal with, especially through classical, hierarchical organisational structures. This article has two aims. The first is an analysis of the tactics of the main actors in cyberconflicts – groups and individuals who attack the penal system and operate in two dimensions: defensive (using information leaks) and offensive (using sabotage). Tactics of the first kind are discussed using the examples of WikiLeaks and the Edaalate Ali group, while tactics of the second kind are discussed using the example of a group of anti-Kremlin hacktivists. The second goal is to present these activities in the broader perspective of network warfare and to propose an outline of the strategy for managing the activities of such actors, which would be based on network "motivational steering", i.e. propaganda stimulation of specific attitudes and grassroots network activities.

Key words: netwar, leaderless resistance, corrections, hacktivism, WikiLeaks, Edaalate Ali

Wstęp

W dynamicznym świecie nowych technologii intensyfikacja działalności radykalnych ugrupowań stosujących nowoczesne metody ideologicznego nacisku, stała się niemałym wyzwaniem – zarówno dla rządów, jak i podmiotów prywatnych. Aktywność tych ugrupowań w cyberprzestrzeni rozpoczęła się co prawda w stosunkowo niedawnej przeszłości, szybko jednak zyskała na intensywności[1]. Nie tylko o intensywność tu jednak chodzi, lecz również o coraz śmielsze i bardziej wyrafinowane podejmowanie skutecznych „działań haktywistycznych" o dwojakim charakterze: informacyjnym oraz ofensywnym. Część tych działań wymierzonych jest w zakłady karne, które dla atakujących stają się często swoistym ideologicznym symbolem (i substytutem zarazem) szeroko rozumianego wymiaru sprawiedliwości. Nie będziemy tu rozstrzygać kwestii moralnego uprawomocnienia haktywistycznych motywacji, skupimy się natomiast

[1] Na temat aktywności ruchu ekologicznego w sieci internetowej patrz: J. Pickerill, *Cyberprotest. Environmental Activism Online*, Manchester University Press, Manchester, New York 2003.

na ogólnej tych motywacji charakterystyce, metodach oraz ocenie skuteczności podejmowanych działań. Całość tych działań rozpatrywana będzie w kontekście szerszego zjawiska, jakim jest walka sieciowa.

Motywowane ideologicznie ataki na system więziennictwa nie miały do tej pory specjalnie spektakularnego charakteru. Ogólnie podzielić je można na: ataki hakerskie nakierowane na pozyskanie informacji (najczęściej o niewłaściwym traktowaniu więźniów czy niehumanitarnych warunkach ich przetrzymywania) oraz ataki, których celem był małoskalowy sabotaż, zwykle połączony z wąsko zakrojoną akcją propagandową. To stosunkowo niewielkie zainteresowanie haktywistów więziennictwem, może skłaniać do myślenia, że system penitencjarny nie jest atrakcyjnym celem dla atakujących bądź też jest on stosunkowo dobrze chroniony. Rzeczywiście, takie myślenie ma pewne podstawy w rzeczywistości. Dla haktywistów o wiele bardziej atrakcyjne są instytucje rządowe czy firmy prywatne o charakterze globalnym, sama zaś ochrona systemów sprawowania kontroli penitencjarnej wydaje się być stosunkowo skuteczna. Nie zmienia to faktu, że i w tym obszarze zdarzają się przypadki prób przełamania tej ochrony. Póki co były to „przełamania" stosunkowo niegroźne oraz, co chyba równie ważne, realizujące w praktyce ideologię humanitaryzmu, w myśl której nie można bezprawnie i z naruszeniem godności więzić czy torturować kogokolwiek. W przyszłości mogą się jednakże zdarzyć przypadki odejścia od humanitarystycznego paradygmatu. Warto o tym pamiętać, przyglądając się skierowanym na system penitencjarny haktywistycznym działaniom w teraźniejszości – tym, w którym wykorzystuje się przede wszystkim zdobyte na drodze haktywizmu informacje, oraz tym, w których elementem wyróżnionym jest „propaganda czynem" oraz wąsko zakrojony sabotaż. Oba te elementy stanowią część większej całości określanej jako walka sieciowa. Zarówno wymienione wyżej działania, jak i sama walka sieciowa będą przedmiotem niniejszego artykułu.

Informacyjne wykorzystanie Internetu

Informacyjny haktywizm w stosunku do systemu penitencjarnego wyrósł przede wszystkim na gruncie moralnego wobec niego sprzeciwu. Grupy haktywistyczne postrzegają zakłady karne jako miejsca systemowej niesprawiedliwości, w których bezkarnie dochodzi do łamania praw człowieka, korupcji i złego traktowania więźniów. Taktyka jest stosunkowo

prosta. Grupy te, wykorzystując systemy monitorujące stosowane przez władze więzienia, włamują się do sieci więziennych, a następnie upubliczniają zdobyte w ten sposób informacje (zwykle o poufnym charakterze). Działania te mają na celu zwrócenie uwagi międzynarodowej społeczności na systemowe nadużycia. Cyberataki należy też uznać za symboliczne akty oporu względem konkretnego, opresyjnego aparatu państwowego, co wpisuje się w szersze antyautorytarne narracje głoszone przez kolektywy haktywistów. Przez strategiczny wyciek poufnych informacji mają oni nadzieję sprawić, że trudniej będzie opór ten zignorować. W taki „informacyjny paradygmat" wykorzystania Internetu wpisuje się aktywność WikiLeaks oraz grupa Edaalate Ali.

WikiLeaks to organizacja założona w 2006 r. przez Juliana Assange. Jej celem jest upublicznianie tajnych dokumentów rządowych oraz materiałów wojskowych ujawniających nadużycia oraz niezgodne z prawem praktyki w stosunku do więźniów. Przez dziesięć lat działalności, na portalu WikiLeaks umieszczono ponad dziesięć milionów dokumentów, z czego obecnie dostępnych jest około trzech tysięcy[2]. Najsłynniejsze opublikowane materiały to między innymi: 1. archiwum dziesiątek tysięcy e-maili z prywatnej poczty elektronicznej byłej sekretarz stanu Hillary Clinton napisanych w czasie trwania jej kampanii prezydenckiej[3]; 2. dostarczone przez Chelsea Manning nagranie z nalotu na Bagdad z 12 lipca 2007 r., zatytułowane Collateral Murder[4], w którym iraccy dziennikarze Reutersa i kilku cywilów ginie w wyniku ostrzału załogi amerykańskiego śmigłowca oraz 3. tajne akta z więzienia wojskowego w Guantamo[5], z których wynika, że władze amerykańskie bezpodstawnie przetrzymywały w więzieniach setki osób z Azji Środkowej, Bliskiego Wschodu, Afryki Północnej i innych miejsc oraz stosowały wobec nich tortury.

Przed sądem wojskowym wspomniany wyżej Manning bardzo długo wyjaśniał kierujące nim ideologiczne motywacje Przyznał się, że będąc żołnierzem armii amerykańskiej, w sposób systematyczny i zaplanowany zbierał tajne materiały wojskowe, do których jako analityk wywiadu w Iraku miał ciągły i niekontrolowany dostęp. Działania rządu i armii amerykańskiej uważał za nieprawidłowe i wymagające reform, a nadziei na to upatrywał w ujawnieniu zebranych informacji opinii publicznej.

[2] https://www.dailydot.com/debug/wikileaks-website-assange-hacked-documents/.
[3] https://wikileaks.org/clinton-emails/,
[4] https://collateralmurder.wikileaks.org/,
[5] https://wikileaks.org/gitmo/or,

Wierzył, że wywoła to narodową debatę na temat właściwego (z moralnego punktu widzenia) prowadzania operacji militarnych, polityki zagranicznej i dyplomatycznej. Zebrane dane, Manning przekazał organizacji WikiLeaks[6], która umożliwia w pełni zanonimizowane dostarczanie informacji przez osoby trzecie. Mogą to być zarówno osoby z wewnątrz organizacji, której dotyczy przeciek (przypadek Manning), jak i osoby z zewnątrz (np. hakerzy z grupy Anonymous, którzy pozyskali, a następnie przekazali WikiLeaks wewnętrzne emaile amerykańskiej agencji wywiadowczej Stratfor). Członkowie organizacji WikiLeaks współpracują z dziennikarzami największych mediów, jak *The New York Times, The Guardian, The Washington Post*, dzięki którym ujawniane informacje zyskują międzynarodowy zasięg (tak stało się również z materiałami przekazanymi przez Manning).

Kolejnym przykładem motywowanych ideologicznie działań o charakterze informacyjnym, jest cyberatak na więzienie Evin w Iranie, zorganizowany przez grupę haktywistów Edaalate Ali[7] (Justice of Iran) w 2021 roku. Niewiele wiadomo na temat członków grupy poza informacjami, których udzielają na stronie internetowej[8], a także na profilach na Telegramie[9], X[10] i Instagramie[11]. Jak piszą o sobie: „Edaalate Ali to grupa haktywistów założona przez irańską młodzież przeciwko reżimowi Islamskiej Republiki Iranu. Rozpoczęliśmy swoją oficjalną działalność w 2011 roku hakując i publikując nagrania z kamer bezpieczeństwa więzienia Evin, które potwierdzają brutalne traktowanie więźniów. Znajdujemy się na pierwszej linii frontu walki z reżimem od momentu jego powstania aż do dziś i będziemy działać aż do jego obalenia. Poza działalnością publiczną w zakresie ujawniania zbrodni reżimu, prowadzimy wiele działań na polu międzynarodowym we współpracy z organizacjami praw człowieka, prasą i innymi instytucjami. Nazwa grupy – Justice of Iran – to to wyraz ironii, wskazujący na nadużywanie przez reżim przekonań religijnych. Reżim, który bez wątpienia zostanie zapisany jako jeden z najokrutniejszych i najbardziej bezwzględnych

[6] Po zebraniu materiałów, Manning skontaktował się z redakcjami The Washington Post i The New York Times, które jednak nie wykazały zainteresowania, dlatego dokumenty trafiły do WikiLeaks, uznanej już wtedy (2010 r.) organizacji, gdzie zostały opublikowane i zyskały międzynarodowy rozgłos.
[7] https://twitter.com/EdaalateAli1400.
[8] https://edaalat.org/home.
[9] https://t.me/EdaalateAli1400.
[10] https://twitter.com/EdaalateAli1400.
[11] http://instagram.com/edaalate_ali_official1/.

w historii ludzkości. Logo grupy przedstawiające niezrównoważoną wagę jest symbolem tej ironii."[12]. Cyberatak na więzienie Evin w Teheranie, w którym przetrzymywani są także więźniowie polityczni, miał na celu ujawnienie przypadków brutalnego traktowania, w tym bezlitosnego bicia więźniów przez strażników więziennych. Motywy stojące za cyberatakiem są jasne, Edaalate Ali dążyła do ujawnienia systemowych niesprawiedliwości i naruszeń praw człowieka, które mają miejsce w irańskim systemie penitencjarnym, rzucając światło na trudną sytuację osób osadzonych w jego murach. Więźniowie (w szczególności polityczni) poddawani są tam arbitralnym zatrzymaniom, torturom i złemu traktowaniu. Publikacja nagrań wywołała międzynarodowe oburzenie i krytykę, skłaniając irańskich urzędników, w tym Mohammada Mehdiego Hajmohammadiego (szefa irańskiego systemu więziennictwa)[13], do oficjalnych przeprosin. Tego rodzaju wydarzenia pokazują, że ujawnienie materiałów międzynarodowej opinii publicznej może być niezwykle skuteczne, a być może w przyszłości przełoży się na zmianę świadomości obywateli, nawet tak represyjnych państw jak Iran.

Konsekwencje opublikowania materiałów o charakterze informacyjnym, takich jak te dotyczące ujawniania przypadków złego traktowania i nadużyć w systemie penitencjarnym, są wieloaspektowe i zależą od kilku czynników, w tym od rodzaju ujawnionych danych, ram prawnych danego kraju oraz motywacji stojących za ich udostępnieniem. Przede wszystkim mogą wzmocnić pozycję dysydentów, aktywistów oraz międzynarodowych organizacji praw człowieka, dostarczając im konkretnych dowodów na poparcie twierdzeń o łamaniu prawa przez rząd. Chociaż ujawnienie nadużyć będzie miało prawdopodobnie pozytywne skutki długoterminowe, może również stanowić bezpośrednie zagrożenie dla zidentyfikowanych za ich pośrednictwem więźniów oraz samego personelu. Reżimy totalitarne mogą bowiem podejmować działania odwetowe wobec dysydentów oraz zastosować wzmożony nadzór i ściślejszą kontrolę informacji. To przekładać się może na zaostrzenie więziennej dyscypliny, zwiększenie kar dla więźniów, a osoby podejrzane o wyciek lub rozpowszechnianie takich informacji mogą spotkać się z poważnymi konsekwencjami. Należy zwrócić uwagę, że społeczność międzynarodowa może tu odegrać kluczową rolę, o ile oczywiście uda jej się zagwarantować, że upublicznienie

[12] https://edaalat.org/about-us.
[13] https://www.bbc.com/news/world-middle-east-58315816.

kompromitujących materiałów doprowadzi do pozytywnych zmian i nie pogorszy trudnej sytuacji osób już cierpiących z powodu represji. Ponadto ujawnione nagrania czy dokumenty mogą zachwiać pozycją rządu nie tylko w sytuacji napiętych stosunków międzynarodowych, ale także wewnętrznie, podważając zaufanie społeczeństwa do danej instytucji. Może to prowadzić do rezolucji, ustanowienia komisji śledczych, a nawet skierowania sprawy do sądów międzynarodowych, takich jak Międzynarodowy Trybunał Karny.

Wycieki informacji są często szeroko komentowane w mediach, kształtując opinię publiczną i wpływając na postrzeganie zaangażowanych osób lub organizacji. Haktywiści, tacy jak WikiLeaks czy Edaalate Ali, dla których istotny jest rozgłos i informowanie o swoich działaniach, wykorzystują do tego media, w tym media społecznościowe. Idzie za tym z reguły duże poparcie społeczne, które przekłada się na rozpoznawalność grupy. Należy zauważyć, że odbiór społeczny może być zróżnicowany – dla niektórych takie działania mają charakter heroiczny, inni postrzegają je jako zdradę zagrażającą bezpieczeństwu narodowemu.

Działania ofensywne w Internecie

Internet może być wykorzystywany także do celów ofensywnych, na przykład do atakowania systemu informatycznego czy danych przeciwnika. Zagrożenie związane z użyciem Internetu przez ideologicznie motywowanych aktywistów było podnoszone wielokrotnie. Barry Collin z Institute for Security and Intelligence in California, który ukuł w latach 80-tych XX wieku termin „cyberterroryzm”[14], opisał w 1997 r. trzy możliwe scenariusze ataków o charakterze cybernetycznym[15]. W jednym ze scenariuszy aktywiści włamują się do systemu komputerowego fabryki płatków śniadaniowych i zwiększają stężenie chemicznych substancji w każdej z paczek. W efekcie dochodzi do licznych zachorowań i śmierci. W drugim scenariuszu destabilizują kraj przez ataki na finansowe

[14] Niektórzy uważają, że termin „cyberterroryzm” pojawił się już w latach 70-tych. Wtedy też z inicjatywy U.S. Air Force powstała pierwsza (zbyt szeroka niestety) definicja cyberterroryzmu: „Użycie informacji i informacyjnego systemu jako broni w konflikcie, gdzie informacje i systemy informacyjne są celami ataków”, patrz: Michael R. Ronczkowski, *Terrorism and Organized Hate Crime- Intelligence Gathering, Analysis. And Investigations*, USA: CRC Press 2003, s. 131–132.

[15] Patrz: H.W. Kushner, *Encyclopedia of Terrosism, Thousend Oaks*, London, New Delhi: Sage Publications, 2003, s. 103.

instytucje oraz giełdę. W trzecim zaatakowany zostaje system kontroli lotniczej, co doprowadza do komunikacyjnego chaosu[16]. Korzyści płynące z posługiwania się cyberatakami jest wiele. 1. W porównaniu ze zwykłym (klasycznym) atakiem jest on stosunkowo tani. Nie trzeba tu wszak stosować materiałów wybuchowych czy innych środków destrukcji, których konstrukcja, przechowywanie, zabezpieczenie, transport są dość kosztowne, nie trzeba też zabezpieczać przedsięwzięcia logistycznie. Do przeprowadzenia ataku wystarczą jedynie umiejętności oraz podłączony do sieci komputer. 2. Cyberaktywizm jest stosukowo bezpieczny dla stosującej go strony[17]. Pozwala na duży stopień anonimowości. Nie ma tu też ryzyka, związanego z poruszaniem się w przestrzeni – brak granic, barier kontrolnych, możliwości bycia rozpoznanym. 3. Daje możliwość „rażenia" stosunkowo dużej liczby podmiotów i wygenerowania olbrzymich strat finansowych, co może skutkować paraliżem i chaosem na dużą skalę i wiąże się z osiągnięciem przez terrorystów ważnego dla nich celu, jakim jest medialność.

W okresach wzmożonych napięć prowadzących do wybuchu wojny między Rosją a Ukrainą różne grupy hakerskie atakowały strony internetowe, sieci rządowe i inną infrastrukturę cyfrową w celu zakłócania ich funkcjonowania. Takie ataki nie ominęły także więzień. Przykładem może być tu zaatakowanie sieci komputerowej rosyjskiego systemu penitencjarnego przez antykremlowskich haktywistów, w ramach odwetu za śmierć lidera opozycji Aleksieja Nawalnego, w rosyjskim więzieniu w Charp, 16 lutego 2024 roku. Jak wynika z przekazanych CNN informacji[18], hakerzy po złamaniu zabezpieczenia sieci komputerowej opublikowali na stronie internetowej jednego z „penitencjarnych kontrahentów" zdjęcie Aleksieja Nawalnego i jego żony, zrobione podczas jednego z antyrządowych protestów oraz tekst: „Niech żyje Aleksiej Nawalny!". Ponadto hakerzy przejęli bazę danych więźniów rosyjskiego reżimu zawierającą dane osobowe kilkuset tysięcy osób, w tym dane na temat kolonii karnej w której przebywał i zmarł Nawalny. Co więcej, hakerzy

[16] Trzeci scenariusz Colinsa został zrealizowany już w 1997 r., kiedy to nastolatek z USA (nieposiadający jednak motywacji politycznych) uzyskał dostęp do sieci telefonicznej małego portu lotniczego w Worcester (Massachusetts) i przerwał komunikację z wieżą kontrolną na kilka godzin.

[17] Jak się ocenia, tylko 5 procent przestępców cyberprzestrzeni zostaje wykrytych i skazanych. Same zaś ataki cybernetyczne rzadko są przez firmy zgłaszane ze względu na przekonanie, że może to popsuć ich wizerunek w oczach klientów. Patrz: Clay Wilson, CRS Report for Congress – Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 29 January, 2008, s. 29, http://www.fas.org/sgp/crs/terror/RL32114.pdf, (1 lutego 2011 r.).

[18] https://kyivindependent.com/cnn-anti-kremlin-hackers-stole-russian-prisoner-database-after-navalnys-death/.

włamali się do sklepu internetowego firmy JSC „Kaluzhskoe", która prowadzi działalność handlową w zakładach karnych w 34 regionach Federacji Rosyjskiej (w tym sklepie rodziny osadzonych mogą kupować potrzebne im produkty). Hakerzy obniżyli ceny wszystkich znajdujących się tam produktów do jednego rubla, a więc znacznie poniżej obowiązujących cen. Przedstawiciele firmy na swojej stronie w mediach społecznościowych zapewniali, że zmiana cen była wynikiem błędu technicznego, a nie ataku hakerów[19]. O antykremlowskich haktywistach wiadomo tylko tyle, że są to osoby różnych narodowości, także rosyjskiej, oraz że łączy je sprzeciw wobec działań Putina, „My, specjaliści IT, opuściliśmy dzisiejszą Rosję", „Kochamy nasz kraj i wrócimy, gdy będzie wolny od reżimu Putina. I będziemy podążać tą drogą do końca", czytamy w wiadomości w języku rosyjskim (na podstawie zrzutu ekranu strony z 18 lutego, sprawdzonym przez CNN)[20] na jednej ze stron internetowych sklepu więziennego.

Walka sieciowa

Koncepcję walki sieciowej (zwanej także „wojną sieciową") opracowali analitycy RAND Corporation, m.in. John Arquilla, David Ronfeldt i Michele Zanini w pracach pt. *The Advent of Netwar, Countering the New Terrorism* oraz *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Twórcy terminu „walka sieciowa" John Arquilla i David Ronfeldt w pracy *The Advent of Netwar* w następujący sposób wyjaśniają to pojęcie: „Termin 'wojna sieciowa' odnosi się do wyłaniającej się formy konfliktu (i przestępczości) na poziomie społecznym, w którym wykorzystywane są środki mniej intensywne niż wojenne oraz sieciowe formy organizacyjne, doktrynalne, strategiczne i komunikacyjne. Strony uczestniczące w konfliktach o takiej formie składają się zazwyczaj z rozproszonych, często małych grup, którym odpowiada komunikacja, koordynacja i działanie w sposób sieciowy, często bez określonego zcentralizowanego przywództwa oraz ośrodków dowodzenia"[21]. Walka sieciowa nie musi odbywać się w sieci internetowej, choć niewątpliwie sieć internetowa jest narzędziem nader często wykorzystywanym. I tak na przykład uczestnicy

[19] https://vk.com/wall-126576485_2535.
[20] https://edition.cnn.com/2024/03/31/politics/navalny-russian-prisoner-database-hack/index.html.
[21] John Arquilla, David Ronfeldt, *The Advent of Netwar*, Santa Monica: RAND Corporation 1996, s. 5–6.

ruchu Anonymous przeprowadzają swoje akcje nie tylko w przestrzeni cyfrowej. Nader często działają w tzw. „realu", aktywizując nie tylko tych, którzy poczuwają się do przynależności do grupy, ale także szerokie masy, zwoływane jednak już za sprawą stron internetowych czy mediów społecznościowych.

Uważa się czasem, że walka sieciowa, z uwagi na wykorzystywanie nie-militarnych środków (m.in. informacji i narzędzi cybernetycznych) oraz zaangażowanie nie-scentralizowanych, społecznie rekrutowanych (czy może lepiej rekrutujących się) jednostek i grup, jest konfliktem o stosunkowo niedużej intensywności. Taka ocena wydaje się co najmniej ryzykowna. Nie uwzględnia ona bowiem ani silnej społecznej mobilizacji, biorącej się z możliwości pozyskiwania „dla sprawy" (dzięki nowym mediom) szerokiego, globalnego wręcz audytorium, ani też wzrastającego znaczenia nowych form organizacyjnych – nowych sieciowych modeli, bardziej bezpiecznych (jeśli brać pod uwagę odporność na inwigilację) i efektywnych (jeśli brać pod uwagę zdolność zadawania wysokich strat przy udziale minimum zaangażowanych środków), niż dotychczasowe hierarchiczne struktury.

„Sieciowe modele" (sieciowe struktury organizacyjne) mogą przyjmować wiele różnych kształtów[22]. Mogą być na przykład powiązane łańcuchowo („chain network"). W takim przypadku komunikacja między poszczególnymi ogniwami (wymiana dóbr i informacji) przebiegać będzie wzdłuż linii ogniw połączonych jedynie ośrodkami sąsiadującymi. Ten typ sieciowej struktury najczęściej spotkać można w gangach przemytniczych. Innym typem powiązań jest sieć węzłowa („hub network"). Tu komunikacja pomiędzy ośrodkami i koordynacja działań uzależniona jest od ośrodka centralnego, od swoistego węzła pośredniczącego, który pełni funkcję przekaźnika informacji i dóbr. Nie jest to jednak komunikacja zorganizowana hierarchicznie. Bywa i tak, że poszczególne ośrodki nic nie wiedzą o swym wzajemnym istnieniu. Ten typ najczęściej spotkać można zarówno w kartelach czy franczyzach, jak i u ugrupowań terrorystycznych. Kolejnym rodzajem powiązań jest sieć wszechkanałową („all-channel network"). W sieci wszechkanałowej wszystkie ośrodki powiązane są ze sobą – każdy z każdym. Nie ma tu jakichkolwiek wyróżnionych węzłów, a komunikacja pomiędzy wybranymi punktami

[22] Patrz J. Arquilla, D. Ronfeldt, "The Advent of Netwar (Revised)", [w:] J. Arquilla, D. Ronfeldt (red.), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica: RAND Corporation 2001.

sieci dokonywać się może niezależnie od wszelkich pozostałych powiązań. Najczęściej ten typ powiązań można odnaleźć wśród wojowniczych ugrupowań (szczególności wśród tzw. „ugrupowań jednej sprawy”[23]), które są w wysokim stopniu zdecentralizowane i zinformatyzowane. Te trzy modele powiązań sieciowych występują również w rozmaitych układach hybrydycznych, łączących w jednej strukturze organizacyjnej dwie lub trzy formy powiązań sieciowych (bądź też nawet sieciowych i hierarchicznych zarazem). Złożone struktury organizacyjne mogą być zróżnicowane na poszczególnych poziomach funkcjonowania – na poziomie najwyższym, dla przykładu, funkcjonować mogą zgodnie z którąś z sieciowych form organizacji, hierarchizując jednocześnie organizację poszczególnych ośrodków sieci, bądź na odwrót. Hierarchiczne struktury organizacyjne mogą też posługiwać się sieciowymi formami organizacji któregoś ze swoich elementów, mogą to robić stale lub doraźnie, w celu np. wykonania jakiegoś zadania, którego nie mógłby sprawnie wykonać organ ustrukturalizowany hierarchicznie, bądź też na odwrót. Możliwości jest wiele. Spośród wszystkich tych prostych czy hybrydycznych form organizacyjnych zdecydowanie najbezpieczniejszą jest sieć wszechkanałowa. Sieci łańcuchowe łatwo jest sparaliżować, przynajmniej czasowo, uderzeniem w którykolwiek z ogniw, sieci węzłowe można zdestruować uderzeniem w ośrodek centralny. Sieć wszechkanałowa, nawet jeśli zostanie w którymś miejscu zaatakowana, nadal może funkcjonować, zapewne też szybko ulegnie regeneracji.

Wojownicze ugrupowania wybierają rzecz jasna różne modele organizacyjne, a czasem nawet rezygnują w ogóle z organizacji w klasycznym rozumieniu tego pojęcia. Tak funkcjonuje m.in. Anonymous, który działa w oparciu o model określany jako „opór bez przywództwa”. Model ten zakłada rezygnację z wszelkich hierarchicznych struktur organizacyjnych, zastępowanych luźną konfiguracją niewielkich, autonomicznych komórek – jednostek bądź małych grup, którymi nie kieruje żaden ośrodek decyzyjny. Działanie takie ma wiele zalet. Jedną z nich jest możliwość odcięcia się od działań niepopularnych czy z różnych względów niepożądanych, pod pretekstem, iż nie spełniają kryteriów ideowych, na przykład wymogu działania bez przemocy, więc nie mogą być uznane za dzieło danej organizacji. „Opór bez przywództwa” pozwala także uznać za „własne dzieło”

[23] Tym mianem określa się zwykle radykalne ugrupowania prozwierzęce (np. Animal Liberation Front), prośrodowiskowe (np. Earth First!) oraz antyaborcyjne (np. Armia Boga).

te ataki, które pasują do przyjętego wzorca działań bezpośrednich (choć w istocie mogły zostać dokonane z całkiem innych powodów). W konsekwencji to rodzaj akcji przesądza o tym, czy dane działanie wpisane zostaje w działalność organizacyjną, czy też nie. Najważniejszą jednak zaletą „oporu bez przywództwa" jest jego aktywistyczna przygodność („efemerycznych aktywistów" nie można inwigilować ani tym bardziej przekupić) oraz masowość (nie trzeba się nigdzie „zapisywać", nikogo znać, każdy może w ramach „oporu" działać lub się wycofać, bez brania na siebie odpowiedzialności).

Uczestnikami wojny sieciowej są ci, którzy w sposób sieciowy realizują swoje cele. Mogą być to zarówno cyberprzestępcy, ideologicznie motywowani haktywiści, ale również ci, którzy w poza internetowej rzeczywistości posługują się w walce sieciowymi strukturami (ekstremiści, terroryści). Jak zauważają John Arquilla i David Ronfeldt: „Wojna sieciowa może być prowadzona zarówno przez „dobrych", jak i „złych" aktorów, a także za pomocą pokojowych, jak i brutalnych środków. Od swoich początków wojna sieciowa wydaje się odpowiednią strategią dla szerokiego przekroju podmiotów niepaństwowych, które starają się stawić czoła władzom państwowym. Etno-nacjonaliści, przestępcy i terroryści – wszyscy znaleźli nową siłę w networkingu"[24]. Uważa się czasem, że walka sieciowa, z uwagi na wykorzystywanie niemilitarnych środków (m.in. informacji i narzędzi cybernetycznych) oraz zaangażowanie niescentralizowanych, społecznie rekrutowanych jednostek i grup, jest konfliktem o stosunkowo niedużej intensywności. Taka ocena nie uwzględnia jednak ani silnej społecznej mobilizacji, biorącej się z możliwości pozyskiwania „dla sprawy" (idei, określonej ideologii) szerokiego, globalnego wręcz audytorium, ani też wzrastającego znaczenia nowych form organizacyjnych – nowych sieciowych modeli (w szczególności oporu bez przywództwa), bardziej bezpiecznych (jeśli brać pod uwagę odporność na inwigilację) i efektywnych (jeśli brać pod uwagę zdolność zadawania wysokich strat przy udziale minimum zaangażowanych środków) niż dotychczasowe hierarchiczne struktury.

[24] J. Arquilla, D. Ronfeld, *The Advent of Netwar (Revisted)*, s. 20, tłumaczenie własne, https://apps.dtic.mil/sti/tr/pdf/ADA485228.pdf

Zakończenie

Omówione w artykule haktywistyczne ataki na zakłady karne były atakami w tak zwanej „słusznej sprawie" – miały na celu zwrócenie uwagi na kwestie społeczne lub polityczne (zwykle ściśle powiązane z nadużyciami prawnymi i złymi warunkami osadzenia). Ich rozprzestrzenianie się stanowi poważne wyzwanie zarówno dla władz więziennych, jak i organów ścigania czy decydentów. Poza bezpośrednim zakłóceniem działalności instytucji ataki te ukazują słabe punkty współczesnej infrastruktury więziennej, wymagające doskonalszych środków cyberbezpieczeństwa i proaktywnych strategii ograniczania ryzyka. Co więcej, ujawnienie domniemanych nadużyć w zakładach karnych wywołało i nadal wywołuje publiczną dyskusję, która prowadzi do zmian w zakresie zarządzania systemem, a nawet reformy całego systemu wymiaru sprawiedliwości. Są to niewątpliwie pozytywne aspekty takich ataków. Jednak te same metody cyberataków stosowane przez haktywistów w „słusznej sprawie" mogą być wykorzystywane przez aktorów o znacznie mniej szlachetnych intencjach. Podwójna natura cyberwojny polega na tym, że narzędzia i techniki opracowane w celu walki o prawa człowieka, mogą zostać wykorzystane do ich podważenia. Przejęcie bazy danych konkretnego więzienia może zostać wykorzystane przez organizacje przestępcze w celu uzyskania dostępu do wrażliwych danych osobowych, prowadząc do kradzieży tożsamości wykorzystywanej często do szantażu. Kiedy haktywiści demonstrują słabości systemów więziennych, nieumyślnie ujawniają je cyberprzestępcom czy organizacjom terrorystycznym. Przeciwnicy ci mogą następnie wykorzystywać te słabe punkty do swoich celów, takich jak organizowanie ucieczek przestępców czy rozpowszechnianie dezinformacji. Co więcej, normalizacja cyberataków jako narzędzia haktywizmu stanowi precedens, który może zachęcić różne podmioty do angażowania się w podobne działania. Granica między haktywizmem a cyberterroryzmem coraz bardziej się zaciera, a to utrudnia wysiłki na rzecz utrzymania bezpieczeństwa cybernetycznego i ochrony krytycznych systemów przed wszelkimi formami ataków. Metody stosowane przez haktywistów mogą zatem stanowić gotowy szablon, z którego korzystać będą cyberterroryści, przekształcając narzędzia wyzwolenia w narzędzia ucisku. To przejście od sprawiedliwego do niesprawiedliwego wykorzystania metod cyberataków ukazuje krytyczny moment w rozważaniach nad etycznym charakterem bezpieczeństwa. Podczas gdy początkowym zamiarem haktywistów jest ochrona praw człowieka i sprawiedliwości w ogóle, szersze

implikacje ich działań wymagają starannego rozważenia długoterminowych konsekwencji. Istnieje pilna potrzeba opracowania kompleksowej strategii, która pozwoli na właściwe (etycznie słuszne) posługiwanie się narzędziami cybernetycznymi, jednocześnie chroniąc społeczeństwo przed ich niewłaściwym wykorzystaniem.

Niezwykle trudno wyobrazić sobie, by walkę ze zdecentralizowanymi, autonomicznymi, sieciowo zorganizowanymi jednostkami lub grupami radykalnymi można było prowadzić za pomocą tradycyjnych metod przeciwdziałania, które opierają się w znacznej mierze na organizacyjnej inwigilacji czy wywiadzie agenturalnym oraz na policyjnych bądź militarnych działaniach operacyjnych. Jest to niemożliwe z dwóch względów. Po pierwsze: po stronie przeciwnika w walkę zaangażowane są siły niehierarchiczne, sieciowe, często zorganizowane na wzór oporu bez przywództwa, z którymi trudno sobie poradzić za pomocą klasycznych, hierarchicznych struktur; po drugie: siły, z którymi przyjdzie walczyć, zespolone są za sprawą walczących idei w wielowęzłową sieć internetową, od istnienia której w gruncie rzeczy zależą.

Pierwszy z wymienionych względów skłania do rozważenia możliwości odejścia od walki z sieciowym aktywizmem wyłącznie za pomocą siły zorganizowanej hierarchicznie. Problem ten zauważyli już pod koniec lat 90-tych XX wieku John Arquilla i David Ronfeld, którzy w tekście poświęconym walce sieciowej, napisali, iż „strukturom hierarchicznym będzie bardzo trudno walczyć z sieciami”[25]. W podobnym tonie wypowiada się Toby Blyth, stwierdzając, że „użycie hierarchicznej siły przeciwko quasi-terrorystycznym sieciom może nie być szczególnie efektywne”[26]. A zatem ci, którzy chcą się obronić przed walką sieciową, muszą przejąć organizacyjny model (opór bez przywództwa) i strategię swoich przeciwników. Wydaje się jednak, że niehierarchiczny model walki jest w praktyce trudny do przeprowadzenia. Trudno sobie bowiem wyobrazić, by siły z natury swej hierarchiczne mogły się przekształcić w swoje przeciwieństwo. Jednak „zaadaptowanie struktur przeciwnika” nie musi się odbywać na drodze prostej transformacji hierarchii w sieci. Hierarchia może wszak wykorzystywać obce sieci do swoich celów. Tak jak mózg posługuje się poszczególnymi częściami ciała, tak hierarchia może zawiadywać sieciami – kierować, kooperować, motywować. Kierowanie, choć jawi się jako dość efektywne działanie,

[25] J. Arquilla, D. Ronfeld, „*The Advent of Netwar: Analytic Background*”, Studies in Conflict & Terrorism, nr 22, 1999, s. 199–200.

[26] T. Blyth, „*Terrorism as Technology: a Discussion of the Theoretical Underpinnings*”, [w:] D. Clarke (red.), *Technology and Terrorism*, New Brunswick, London: Transaction Publischers, 2004, s. 45.

zawsze będzie miało relatywnie ograniczony zasięg, co nie oznacza, że nie może być do pewnego stopnia skuteczne. Kooperacja (przykładem może być tu współpraca pomiędzy organizacjami typu „watchdog" a rządem Stanów Zjednoczonych) ma swoje ograniczenia formalne i też nie obejmie całego pola walki. Największe nadzieje należy, naszym zdaniem, pokładać w „zawiadywaniu motywacjami", czyli propagandowym pobudzaniu do określonych postaw i działań oddolnych, przekładających się na działania sieciowe. W takim zawiadywaniu można wykorzystywać różnorodne techniki, obecne już od dawna w działaniach ekonomiczno-marketingowych (np. astroturfing[27]) czy propagandowych (mentalne kształtowanie postaw przez ukazanie atrakcyjności ideologicznej danej sprawy). Oczywiście, wobec tego rodzaju technik zgłasza się często zastrzeżenia, które mogą do nich zniechęcać demokratyczne i humanistycznie zorientowane hierarchie (a przynajmniej chcące za takowe uchodzić). W nowoczesnych społeczeństwach nie są to bowiem działania pochwalane moralnie. Nie wydaje się jednak, by istniało inne skuteczne rozwiązanie.

[27] Działania nazywane astroturfingiem polegają zwykle na udawaniu przez niewielką grupę ludzi rzeszy aktywistów lub konsumentów w zamiarze zyskania poparcia społecznego dla danej idei lub zdyskredytowanie jej. „Astroturfing is an artificially-manufactured political movement designed to give the appearance of grassroots activism. It involves presenting a biased or skewed view of public opinion as if it were a genuine, grassroots movement, when in fact it is a coordinated effort by a small group of individuals or organizations. Unlike natural grassroots campaigns which are people-rich and money-poor, an astroturf campaign tends to be the opposite, well-funded but with little actual support from voters." Astroturf. (2017). Downloaded from: https://politicaldictionary.com/words/astroturfing/.

Bibliografia

Arquilla J., Ronfeldt D., *The Advent of Netwar*, Santa Monica: RAND Corporation 1996.

Arquilla J., Ronfeldt D., *The Advent of Netwar: Analytic Background*, Studies in Conflict & Terrorism, nr 22, 1999.

Blyth T., *Terrorism as Technology: a Discussion of the Theoretical Underpinnings* [w]: D. Clarke (red.), *Technology and Terrorism*, New Brunswick, London: Transaction Publishers 2004.

Coleman G., *Hacker, hoaxer, whistleblower, spy. The many faces of anonymous* Verso. London. New York 2014.

Chen T.M., *Cyberterrorism after stuxnet* [dostęp: 03.02.2024]. Strategic Studies Institute and U.S. Army War College Press 2014. Tekst jest dostępny: https://www.files.ethz.ch/isn/180822/pub1211.pdf.

Gajewski T., *Asymetria w polityce bezpieczeństwa Islamskiej Republiki Iranu* [w:] W. Sokała, B. Zapała (red.), *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, Warszawa 2011.

Greenberg A., *Sandworm. Nowa era cyberwojny i polowanie na najbardziej niebezpiecznych hakerów Kremla*. PWN 2021.

Kushner H.W., *Encyclopedia of Terrosism*, Thousend Oaks, London, New Delhi: Sage Publications 2003.

Jordan D.A., *US Intelligence Law: A Comprehensive Multimedia Introduction.* United States of America 2010

Lewis J.A., *Cyber Terror: Missing in Action* [w:] D. Clarke (red.), *Technology and Terrorism*, New Brunswick, London: Transaction Publishers 2004.

Lia B*., Globalisation and the Future of Terrorism. Patterns and Predictions*, London, New York, Routledge 2005.

Marighella C., *Minimanual of the Urban Guerilla*, Boulder: Paladin Press 1975. Tekst jest dostępny: http://www.latinamericanstudies.org/marighella.htm.

Pickerill J., Cyberprotest. *Environmental Activism Online*, Manchester, New York: Manchester University Press 2003.

Ronczkowski M.R., *Terrorism and Organized Hate Crime- Intelligence Gathering, Analysis. And Investigations*, USA: CRC Press 2003.

Verton D., *Black Ice. Niewidzialna ręka cyberterroryzmu*, Gliwice 2004.

Źródła internetowe:

Arquilla J., Ronfeldt D., *The Advent of Netwar (Revisited)* https://apps.dtic.mil/sti/tr/pdf/ADA485228.pdf [dostęp: 06.03.2024]

Arquilla J., Ronfeldt D., *Swarming and the Future of Conflict*, Santa Monica: RAND National Defense Research Institute 2000. http://www.analytictech.com/mb021/swarming%20DB311.pdf [18.02.2011].

Arquilla J., Ronfeldt D., *Networks and Netwar*, http://radio-weblogs.com/0107127/stories/2002/09/10/networksAndNetwar.html [dostęp: 19.02.2011].

Booth K., Dunne T. (red.), *Worlds in Collision: Terrorism and the Future of Global Order*, Houndsmill, Basingstoke: Pagrave 2002.

Conway M., *Reality Bites: Cyberterrorism and the Terrorist 'Use' of the Internet*, First Monday, 2002, t. 7, nr 11, http://doras.dcu.ie/498/1/first_mon_7_11_2002.pdf [dostęp: 29.01.2011].

Edwards S.J.A., *Swarming on the Battlefield: Past, Present, and Future*, Rand Corporation 2000. http://www.rand.org/pubs/monograph_reports/MR1100.html [dostęp:16.02.2011].

Espiner T., *Security Expert: Storm Botnet 'services' Could Be Sold*, CnetNews.com, 16.10.2007, https://www.cnet.com/news/privacy/security-expert-storm-botnet-services-could-be-sold/ [dostęp: 12.06.2008].

Graff G., *America's Top Spy Talks Snowden Leaks and Our Ominous Future*, Wired, 17.11.2016, https://www.wired.com/2016/11/james-clapper-us-intelligence/ [dostęp: 12.02.2024]

Greenwald G., MacAskill E., Poitras L., *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, The Guardian, 11.06.2013, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [dostęp: 12.02.2024].

Lemos R., *Bot software looks to improve peerage*, The Register, 4.05.2006, https://www.theregister.com/2006/05/04/nugache_p2p_botnet/ [dostęp: 16.07.2008].

Lewis J. A. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Threats*, December 2002 http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf [dostęp: 9.02.2011].

Łącki B., *Botnet od podszewki*, 13.06.2007, Heise Security, http://www.heise-online.pl/security/features/Botnet-od-podszewki-778119.html [dostęp: 12.02.2011].

Nazario J., *Georgia DDoS Attacs – A Quick Summary of Observations*, 12.08.2008, http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of--observations/ [dostęp: 24.03.2008].

Scharre P., *Unleash the Swarm: the Future of Warfare. War on the Rocks*, 04.03.2015, https://warontherocks.com/2015/03/unleash-the-swarm-the-future-of-warfare/ [dostęp: 3.03.2024].

Thalen M., *WikiLeaks website is struggling to stay online–as millions of documents disappear*, 22.11.2022, daily dot, https://www.dailydot.com/debug/wikileaks-website-assange-hacked-documents/ [dostęp: 08.02.2024]

The Spiegel, *New NSA Revelations. Inside Snowden's Germany File*, 18.06.2014, https://www.spiegel.de/international/germany/new-snowden-revelations-on-nsa-spying-in-germany-a-975441.html [dostęp: 12.02.2024].

The Spiegel, *The NSA in Germany. Snowden's Documents Available for Download*, 18.06.2014, https://www.spiegel.de/international/the-germany-file-of-edward-snowden-documents-available-for-download-a-975917.html [dostęp 10.02.2011].

WikiLeaks, *Collateral Murder*, 05.04.2010, https://collateralmurder.wikileaks.org/ [dostęp: 10.02.2024]

WikiLeaks, *GitmoFiles, WikiLeaks Reveals Secret Files on All Guantánamo Prisoners*, https://wikileaks.org/gitmo/ [dostęp: 10.02.2024]

WikiLeaks, *Hillary Clinton Email Archive*, 16.03.2016 [dostęp: 10.02.2024]

Waterman S., *Cyber War: Who Cyber Smacked Estonia*, 11.06.2007, Space War. http://www.spacewar.com/reports/Who_Cyber_Smacked_Estonia_999.html [dostęp: 10.02.2011].

Wilson C., *CRS Report for Congress – Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, 29 January, 2008, http://www.fas.org/sgp/crs/terror/RL32114.pdf [dostęp: 1.02.2011].